UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,465	01/12/2006	Yujiro Ito	450100-05166	7460

7590 07/07/2009

William S Frommer
Frommer Lawrence & Haug
745 Fifth Avenue
New York, NY 10151

EXAMINER	
SHOLEMAN, ABU S	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
07/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,465	ITO ET AL.	
	Examiner	Art Unit	
	ABU SHOLEMAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-20 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 May 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending and claims 10 and 21 are cancelled.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 9, 11-14 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lynn (5345508) (hereinafter Lynn) in view of Jaechul et al (Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation 2002) (hereinafter Jaechul) and further in view of Gligor et al (US 20020048364)(hereinafter Gligor).

As per claim 1, Lynn discloses "An encryption apparatus, comprising: hold means for holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, lines 36-39, Fig 2 [22] , Cache holds data according to reset signal and column 5, lines 1-2, reset signal generated new sequence of data);

"one or a plurality of counters that count up or count down the count values with a the trigger signal and reset the count values to predetermined values with the reset

signal" as (column 6, lines 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero);

"a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means" as (column 5, lines 12-15 the cipher text output information is transmitted to receiver through a channel);

"signal generation means for generating the trigger signal and the rest signal supplied to the hold means and the one or plurality of counters according to a second predetermined rule and or at predetermined timing" as (column 6, lines 3-10, reset signal generates new IV according to counter that has been described as a plaintext data sequence counter according to a clock function).

But Lynn fails to disclose "encryption means for reading the data held by the hold means and one or a plurality of the count values and for encrypting the data held by the hold means and one or a plurality of the count values of the one or plurality of counters";

"calculation means for calculating the output of the encryption means and input data that are input from the outside according to a first predetermined rule, encrypting the input data and outputting the encrypted data);

However, Jaechul discloses "encryption means for reading the data held by the hold means and one or a plurality of the count values and for encrypting the data held by the hold means and one or a plurality of the count values of the one or plurality of counters" as (on page 109, lines 23-24, CTR-CFB, function [f] has hold data [lsb]

concatenation with counter [any number of counter] and encrypting the held data with counter);

"calculation means for calculating the output of the encryption means and input data that are input from the outside according to a first predetermined rule, encrypting the input data and outputting the encrypted data" as (on page 109, lines 23-24, Xi is inputed from outside to XORed with function [f] and on page 113, Fig 2, y1 is outputed to next hold means with incremented of counter);

Lynn and Jaechul are analogous arts because they are same field of endeavor of the method of data encryption.

Therefor, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including the counter-cipher feedback mode that is taught by Jaechul because it would provide higher resistance against practical attacks.

The combination of Lynn and Jaechul fail to disclose wherein the encryption means reads in parallel the data held by hold means, one or a plurality of the count values, and a key outputted by the signal generation means, and

wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data.

However, Gligor discloses wherein the encryption means reads in parallel the data held by hold means, one or a plurality of the count values (Fig. 9, numeral 53 reads x1 data and r01 counter in parallel), and a key outputted by the signal generation means (Fig 9, K is outputted by signal), and

wherein the input data is sequentially inputted to the calculation means in a predetermined unit (Fig 9, data x1...x4, x5-x8, x7- x12 are sequentially inputted into numeral 53 of plaintext segment 1, segment 2, and segment 3 respectively, each segment is a predetermined unit of data), and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data (Fig 9, data can be reset in numeral 27 of each plaintext segment by initializing x for new data, wherein each segment will not be affecting encryption of next new segments of data).

Therefor, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Jaechul by including a parallel block encryption that is taught by Gligor because it would provide both data confidentiality and integrity with a single cryptographic primitive and a single processing pass over the input plaintext.

As per claim 2, Lynn in view Jaechul in view of Gligor disclose "wherein a fixed value is input to the encryption means" as (Jaechul, on page 109, lines 20-25, fixed value (lsb [yi-1]) is inputed into encryption function), and "wherein the encryption means

encrypts the fixed value, the data held by the hold means, and the one or plurality of count values" as (Jaechul, on page 113, Fig 2, encrypt hold value v-bit and counter+2).

As per claim 3, Lynn in view of Jaechul in view of Gligor disclose "Wherein the reset signal that resets the data held by the hold means is supplied to the hold means at timing in synchronization with the reset signal supplied to at least one of the one or plurality of counters" as (Lynn, column 5, lined 1-5, reset signal that a new sequence is to be generated for cache [22] and column 6, lines 5-10, counter[21] has been described with respect to Fig 2 as a plaintext data [32] sequence counter).

As per claim 9, this claim is directed to an encryption method and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 11, this claim is directed to a record medium and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 12, Lynn discloses "A decryption apparatus that decrypts encrypted data encrypted by an encryption apparatus" as (column 6, lines 30-35 and Fig 3, receiver decode the ciphertext to plaintext), the decryption apparatus comprising:

hold means for holding a part or all input data with a trigger signal and resetting the held data with a reset signal" as (column 5, lines 36-39, Fig 2 [22] , Cache holds

data according to reset signal and column 5, lines 1-2, reset signal generated new sequence of data);

"one or a plurality of counters that count up or count down the count values with a the trigger signal and reset the count values to predetermined values with the reset signal" as (column 6, lines 5-7, counter is decrementing with each sequence processed and line 2, counter contents reaches zero);

"a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means" as (column 5, lines 12-15 the cipher text output information is transmitted to receiver through a channel);

"signal generation means for generating the trigger signal and the rest signal supplied to the hold means and the one or plurality of counters according to a second predetermined rule and or at predetermined timing" as (column 6, lines 3-10, reset signal generates new IV according to counter that has been described as a plaintext data sequence counter according to a clock function).

But Lynn fails to disclose "encryption means for reading the data held by the hold means and one or a plurality of the count values and for encrypting the data held by the hold means and one or a plurality of the count values of the one or plurality of counters";

"calculation means for calculating the output of the encryption means and input data that are input from the outside according to a first predetermined rule, encrypting the input data and outputting the encrypted data);

However, Jaechul discloses "encryption means for reading the data held by the hold means and one or a plurality of the count values and for encrypting the data held by the hold means and one or a plurality of the count values of the one or plurality of counters" as (on page 109, lines 23-24, CTR-CFB, function [f] has hold data [lsb] concatenation with counter [any number of counter] and encrypting the held data with counter);

"calculation means for calculating the output of the encryption means and input data that are input from the outside according to a first predetermined rule, encrypting the input data and outputting the encrypted data" as (on page 109, lines 23-24, Xi is inputed from outside to XORed with function [f] and on page 113, Fig 2, y1 is outputed to next hold means with incremented of counter);

Lynn and Jaechul are analogous arts because they are same field of endeavor of the method of data encryption.

Therefor, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn by including counter-cipher feedback mode that taught by Jaechul because it would provide higher resistance against any attack in computer security system.

the combination of Lynn and Jaechul fail to disclose wherein the encryption means reads in parallel the data held by hold means, one or a plurality of the count values, and a key outputted by the signal generation means, and

wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data.

However, Gligor discloses wherein the encryption means reads in parallel the data held by hold means, one or a plurality of the count values (Fig. 9, numeral 53 reads x1 data and r01 counter in parallel), and a key outputted by the signal generation means (Fig 9, K is outputted by signal), and

wherein the input data is sequentially inputted to the calculation means in a predetermined unit (Fig 9, data x1…x4, x5-x8, x7- x12 are sequentially inputted into numeral 53 of plaintext segment 1, segment 2, and segment 3 respectively, each segment is a predetermined unit of data), and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data (Fig 9, data can be reset in numeral 27 of each plaintext segment by initializing x for new data, wherein each segment will not be affecting encryption of next new segments of data).

Therefor, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Jaechul by including a parallel block encryption that is taught by Gligor because it would provide both data confidentiality and integrity with a single cryptographic primitive and a single processing pass over the input plaintext.

As per claim 13, Lynn in view Jaechul disclose "wherein a fixed value is input to the encryption means" as (Jaechul, on page 109, lines 20-25, fixed value (lsb [yi-1]) is inputed into encryption function), and "wherein the encryption means encrypts the fixed value, the data held by the hold means, and the one or plurality of count values" as (Jaechul, on page 113, Fig 2, encrypt hold value v-bit and counter+2).

As per claim 14, Lynn in view of Jaechul discloses "Wherein the reset signal that resets the data held by the hold means is supplied to the hold means at timing in synchronization with the reset signal supplied to at least one of the one or plurality of counters" as (Lynn, column 5, lined 1-5, reset signal that a new sequence is to be generated for cache [22] and column 6, lines 5-10, counter[21] has been described with respect to Fig 2 as a plaintext data [32] sequence counter).

As per claim 20, this claim is directed to a decryption method and contains limitations that are substantially similar to those recited in claim 12 above, and accordingly is rejected for similar reasons.

As per claim 22, this claim is directed to a record medium and contains limitations that are substantially similar to those recited in claim 20 above, and accordingly is rejected for similar reasons.

4. Claims 4-5 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lynn (5345508) (hereinafter Lynn) in view of Jaechul et al (Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation 2002) (hereinafter Jaechul) and further in view of Tehranchi (Patent No: 7242772 B1) (hereinafter Tehranchi).

As per claim 4, Lynn in view of Jaechul disclose all the limitations as set forth above; Lynn in view of Jaechul fails to disclose "wherein the input data are picture data, and wherein the reset signal that resets the hold means is in synchronization with the picture data".

However, Tehranchi discloses "wherein the input data are picture data" as (column 1, lines 58-64, motion picture data for encrypted, and "wherein the reset signal that resets the hold means is in synchronization with the picture data" as (column 3, lines 16-19, synchronize key to the data, where key is generated by reset signal for each new sequence of picture data).

Lynn in view of Jaechul and Tehranchi are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Jaechul by including a picture data instead of plaintext that taught by Tehranchi in order to prevent the data piracy of digital motion pictures (column 1, line 25-28).

As per claim 5, Tehranchi discloses "wherein the reset signal that resets the hold means is in synchronization with each line of the picture data" as (column 5, lines 26-29, encryption key assigned to each said single data block and a block synchronization index indicating a correspondence between said encryption key [Lynn discloses in Fig 2, reset signal with key[12]] and said single data block).

As per claim 15, this claim is directed to a decryption apparatus and contains limitations that are substantially similar to those recited in claim 4 above, and accordingly is rejected for similar reasons.

As per claim 16, this claim is directed to a decryption apparatus and contains limitations that are substantially similar to those recited in claim 5 above, and accordingly is rejected for similar reasons.

5. Claims 6-8 and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lynn (5345508) (hereinafter Lynn) in view of Jaechul et al (Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation 2002) (hereinafter Jaechul) and further in view of Hosford (5966450 B1) (hereinafter Hosford).

As per claim 6, Lynn in view of Jaechul disclose all the limitations as set forth above; Lynn in view of Jaechul fail to disclose "wherein the input data are picture data and wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the picture data".

However, Hosford discloses "wherein the input data are picture data" as (column 2, lines 61-63, frames of data are inputed for encryption) and "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with the picture data" as (Column 3, lines 51-55, resetting the frame counter that is transmitted with frame).

Lynn in view of Jaechul and Hosford are analogous arts because they are the same field of endeavor of apparatus of encryption of data stream.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Lynn in view of Jaechul by including resetting the frame counter that taught by Hosford because it would improved unauthorized decryption.

As per claim 7, Hosford discloses "wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each frame of the picture data" as (column 3, line 51-55, resetting the frame counter comprises setting the frame counter to the stored initial value and frame counter is synchronization with each other).

As per claim 8, Hosford discloses " wherein the reset signal that resets at least one of the one or plurality of counters is in synchronization with each line of the picture

data" as (column 3, line 3-5, frame on a bit-by bit basis to produce en encrypted frame).

As per claim 17, this claim is directed to a decryption apparatus and contains limitations that are substantially similar to those recited in claim 6 above, and accordingly is rejected for similar reasons.

As per claim 18, this claim is directed to a record medium and contains limitations that are substantially similar to those recited in claim 7 above, and accordingly is rejected for similar reasons.

As per claim 19, this claim is directed to a record medium and contains limitations that are substantially similar to those recited in claim 8 above, and accordingly is rejected for similar reasons.

Examiner Notes

6. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the

references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

7. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

8. The following reference teaches execution of trial data.

US 20020048364

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 28, 2009

Abu Sholeman
Examiner
Art unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437